Vendor Landscape: Endpoint Protection

Find anti-malware and more, now wrapped up in a fully-fledged suite.

INFO~TECH
RESEARCH GROUP

Introduction

Endpoint protection has featured too many standalone options for too long. Vendors are starting to recognize the value of consolidating capabilities.

This Research Is Designed For:

✓Enterprises seeking to select a solution for endpoint protection.

✓Their endpoint protection use case may include:

- Enterprises looking for a centrally managed solution that will provide protection for a variety of devices from laptops to mobile devices.
- Enterprises that are migrating from standalone capabilities like DLP or WCF, to a consolidated solution.

This Research Will Help You:

✓Understand what's new in the endpoint protection market.

✓Evaluate endpoint protection vendors and products for your enterprise needs.

✓Determine which products are most appropriate for particular use cases and scenarios.

Market overview

How it got here

- Threat complexity increased from the first 1980s' attacks like Melissa and Love Bug, first with polymorphic viruses, and more recently, Advanced Persistent Threats (APTs) affecting both large-scale organizations, as seen in news headlines, and regular organizations.
- To combat these threats, the first commercial anti-virus scanners were released in the early '90s. Over time, these early tools gained an inordinate number of competitors. Tools themselves have added capability after capability as the malware writers evolve their craft and push the bounds of what viruses, worms, and other malware can do.
- In the past, it was customary to have standalone solutions for anti-malware, encryption, and more, but as the landscape became more complicated, organizations needed a streamlined way to manage their solutions, while also offering the same robust security capabilities.

Where it's going

- Similar to most security solutions, the movement has been in the direction of increased consolidation. Endpoint anti-malware solutions and endpoint encryption solutions have now become comprehensive endpoint protection suites, wrapping up other data-related and content control security capabilities such as:
  - Removable device content control
  - Removable media encryption
  - URL filtering/web control
- With APTs not going away any time soon, organizations are recognizing the need to take a proactive and holistic approach to their security. Vendors can expect to find more ways to consolidate and provide single pane-of-glass central management.

Info-Tech Insight

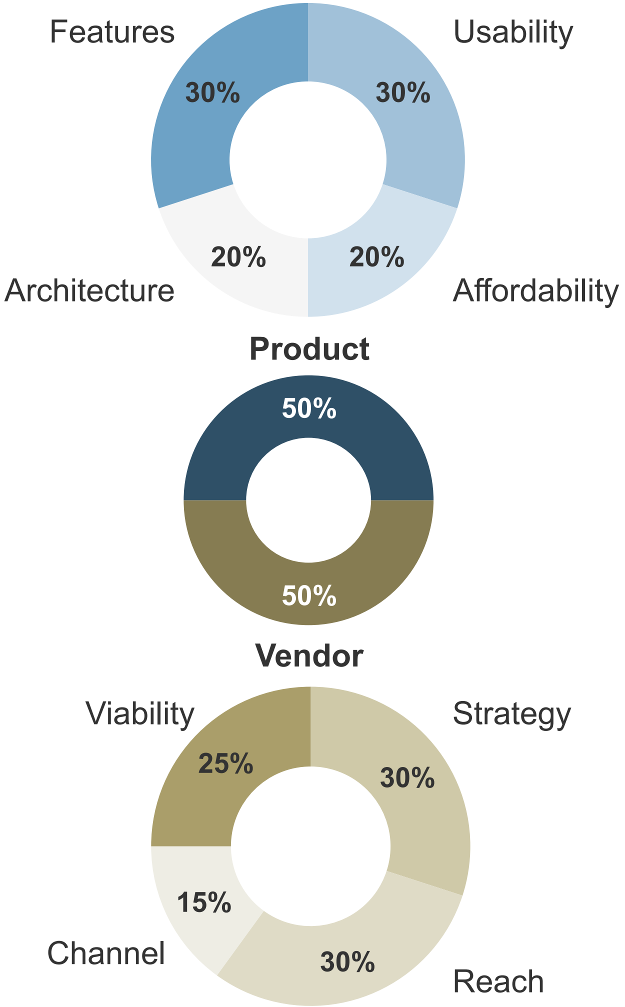
As the market evolves, capabilities that were once cutting edge become default and new functionality becomes differentiating. Full disk encryption has become a Table Stakes capability and should no longer be used to differentiate solutions. Instead focus on removable device content control and removable media encryption to get the best fit for your requirements.

Endpoint Protection criteria & weighting factors

Product Evaluation Criteria	
Features	The solution provides basic and advanced feature/functionality.
Usability	The end-user and administrative interfaces are intuitive and offer streamlined workflow.
Affordability	Implementing and operating the solution is affordable given the technology.
Architecture	Multiple deployment options and extensive integration capabilities are available.

Vendor Evaluation Criteria	
Viability	Vendor is profitable, knowledgeable, and will be around for the long term.
Strategy	Vendor is committed to the space and has a future product and portfolio roadmap.
Reach	Vendor offers global coverage and is able to sell and provide post-sales support.
Channel	Vendor channel strategy is appropriate and the channels themselves are strong.

Criteria Weighting



The Info-Tech Endpoint Protection Vendor Landscape

The zones of the Landscape

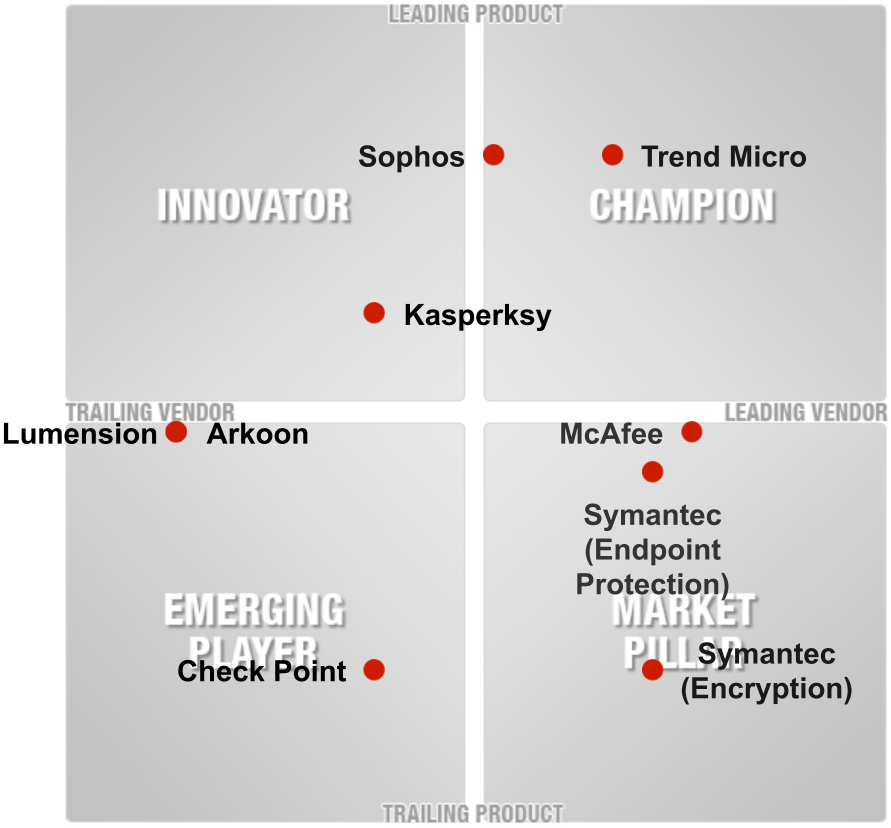
Champions receive high scores for most evaluation criteria and offer excellent value. They have a strong market presence and are usually the trend setters for the industry.

Market Pillars are established players with very strong vendor credentials, but with more average product scores.

Innovators have demonstrated innovative product strengths that act as their competitive advantage in appealing to niche segments of the market.

Emerging Players are comparatively newer vendors who are starting to gain a foothold in the marketplace. They balance product and vendor attributes, though score lower relative to market Champions.

The Info-Tech Endpoint Protection Vendor Landscape

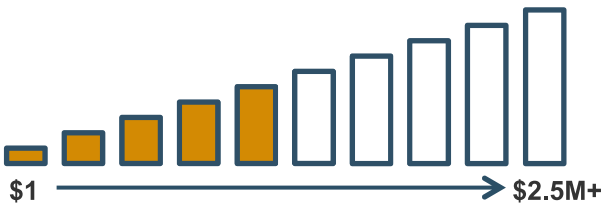


Trend Micro offers the full package in endpoint protection

Champion

Product:	Smart Protection for Endpoints
Employees:	5,217
Headquarters:	Tokyo, Japan
Website:	trendmicro.com
Founded:	1988
Presence:	TYO:4704

3 year TCO for this solution falls into pricing tier 5, between $50,000 and $100,000



Pricing provided by vendor

Overview

- One of the largest endpoint security providers, Trend Micro offers comprehensive advanced threat and data protection for desktops to mobile devices.

Strengths

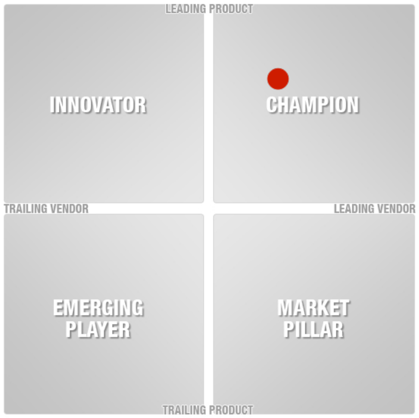
- Trend Micro's Smart Protection for Endpoints offers one of the strongest advanced feature sets of the solutions evaluated, including removable device content control and URL filtering and web control.
- The product has one of the most interactive and intuitive interfaces. It offers user-centric visibility which means admins can see all users in the environment and the devices/end points associated with them. Finally, it offers hybrid cloud management and licensing.

Challenges

- Trend Micro has recently been looking to improve their partner program. To address this, they are launching a new program in July 2014.

Even from a vendor standpoint, Trend Micro is one of the strongest players

Vendor Landscape



Value Index

59

2nd out of 9

Product					Vendor				
Overall	Features	Usability	Afford.	Arch.	Overall	Viability	Strategy	Reach	Channel
●	●	●	◑	●	◕	●	◕	●	◕

In Alignment With Your Organization's Overall Security Strategy and Infrastructure

Data Loss Prevention Strategy ✓	Cloud-Based Deployment ✓
Vulnerability/System Management Strategy ✓	On-Premise Deployment ✓

- Trend Micro Smart Protection for Endpoints can encrypt folders and any files that fall into those folders as well as removable media.
- The integrated DLP provides visibility and control of data to and from USB ports, CD/DVDs, LPT ports, removable disks, cloud syncing applications, etc. Also collaborates with other Trend Micro security solutions.
- The vulnerability protection provides virtual patch deployment and zero-day protection.
- The application control provides whitelisting via cloud-based categories and system lockdown.
- Trend Micro offers both on-premise and cloud-based options for organizations.

Features

FFE	Encryption	Content	Port Control	Patch Mgmt.	App White	URL	Cloud
●	●	●	●	●	●	●	●

Info-Tech Recommends:

Organizations looking for a comprehensive and affordable solution will find all of their requirements met with Trend Micro's Smart Protection for Endpoints. Not only does it have a full feature set, it also has an interactive interface; it is an ideal option for a wide range of organizations.

This highly consolidated security suite helps enhance your overall risk management capabilities

Only one vendor evaluated had all of the advanced features as part of its endpoint protection product.

1 **Enhanced risk management**

2

3

Why Scenarios?

In reviewing the products included in each Vendor Landscape^{TM}, certain use cases come to the forefront. Whether those use cases are defined by applicability in certain locations, relevance for certain industries, or as strengths in delivering a specific capability, Info-Tech recognizes those use cases as Scenarios, and calls attention to them where they exist.

Exemplary Performers

TREND MICRO

Trend Micro offers a complete advanced features set, including removable media encryption, removable device content control, port control, patch management, and more. The product's robustness is indicative that Trend Micro is recognizing the ever-changing needs of its customers and addressing them in a comprehensive solution that also scores high in overall usability.

Data is no longer static and solutions must protect it now that it is often in transit

Solutions with removable device content control and removable media encryption are equipped to deal with data on the move.

1

2 Removable device control

3

Why Scenarios?

In reviewing the products included in each Vendor Landscape^{TM}, certain use cases come to the forefront. Whether those use cases are defined by applicability in certain locations, relevance for certain industries, or as strengths in delivering a specific capability, Info-Tech recognizes those use cases as Scenarios, and calls attention to them where they exist.

Both features

ARKOON NETWORK SECURITY

Lumension IT Secured. Success Optimized.

SOPHOS

Symantec (Endpoint Protection)

Symantec (Endpoint Encryption)

TREND MICRO

Removable media encryption only

Check Point SOFTWARE TECHNOLOGIES LTD.

KASPERSKY lab

Removable device content control only

McAfee An Intel Company

Organizations need solutions that can integrate with more than one platform, especially with mobile devices in the mix

Solutions that can work with different operating systems *and* a variety of mobile devices will be more attractive in today's diverse landscape.

1

2

3 **Platform integration**

Why Scenarios?

In reviewing the products included in each Vendor Landscape^{TM}, certain use cases come to the forefront. Whether those use cases are defined by applicability in certain locations, relevance for certain industries, or as strengths in delivering a specific capability, Info-Tech recognizes those use cases as Scenarios, and calls attention to them where they exist.

All (Windows, Mac, mobile devices)

KASPERSKY lab

SOPHOS

McAfee
An Intel Company

TREND MICRO

Windows/Mac

Symantec
(Endpoint Protection)

Symantec
(Endpoint Encryption)

Windows only

ARKOON
NETWORK SECURITY

Lumension
IT Secured. Success Optimized.

Check Point
SOFTWARE TECHNOLOGIES LTD.

Table Stakes represent the minimum standard; without these, a product doesn't even get reviewed

The Table Stakes

Feature	What it is:
Signature-based & behavioral anti-malware	Black-listing, white-listing, and pattern-matching abilities – the essence of AV.
Signature-based & behavioral anti-spyware	Recognition, restriction, and removal of information gathering software.
Host IPS	Ability to actively recognize and respond to inappropriate inbound traffic.
Host FW	Rules-based control of the traffic and actions allowed at the endpoint.
Full-disk encryption	Offers full-disk option that encrypts the entire physical disk as opposed to specific files or folders.

What does this mean?

The products assessed in this Vendor Landscape™ meet, at the very least, the requirements outlined as Table Stakes.

Many of the vendors go above and beyond the outlined Table Stakes, some even do so in multiple categories. This section aims to highlight the products' capabilities **in excess** of the criteria listed here.

Info-Tech Insight

If Table Stakes are all you need from your endpoint protection solution, the only true differentiator for the organization is price. Otherwise, dig deeper to find the best price to value for your needs.

Advanced Features are the capabilities that allow for granular market differentiation

Scoring Methodology

Info-Tech scored each vendor's features offering as a summation of its individual scores across the listed advanced features. Vendors were given one point for each feature the product inherently provided. Some categories were scored on a more granular scale with vendors receiving half points.

Advanced Features

Feature	What we looked for:
File/folder encryption	Protection for files and folders wherever they're stored – laptops, desktops, mobile devices, etc.
Removable media encryption	Ability to encrypt removable devices such as USB devices, etc. Devices can be used on other workstations without other software.
Removable device content control	Integrated DLP capabilities, allowing for control and policing of data as it moves to and from removable devices.
Port control	Refers to ability to control whether USB ports are active or not.
Patch mgmt.	Capability to identify what kind of patches are missing. Can control how to patch systems.
Application whitelisting	Allow a user or admin the ability to grant permission to particular applications in order for them to run.
URL filtering/web control	Blocking of web traffic that may be harmful, offensive, or legally inappropriate.
Cloud deployment options	Availability of opportunity to deploy endpoint protection in the cloud.

Executive summary

Info-Tech evaluated nine competitors in the endpoint protection market, including the following notable performers:

Champions:

- **Trend Micro** has a total package of fully advanced features and a decent price amongst competitors.

Info-Tech Insight

1. **Protect data on the move:**

   Most devices in today's workplace are mobile, so protection can no longer be static. Removable device encryption and content control must extend beyond laptops to USB and mobile devices to ensure holistic protection.

2. **Interfaces need to be interactive:**

   With the myriad of information that admins must parse through on a daily basis, it's imperative that today's endpoint solutions – as they consolidate multiple capabilities under one view – be seamless and straightforward, with the ability to monitor activities and do deeper dive analysis in real time.

3. **Expanded platform integration is key:**

   It's no longer acceptable for products to simply be compatible with Windows. They also need to work with Mac, Linux, and mobile platforms.

Endpoint Protection vendor selection / knock-out criteria: market share, mind share, and platform coverage

- Endpoint Protection reflects an ever-consolidating market of security tools. Wrapping up anti-malware, web content filtering, and other capabilities into one centrally managed solution demonstrates that today's customers want an all-in-one option for their endpoints.
- For this Vendor Landscape, Info-Tech focused on those vendors that offer broad capabilities across multiple platforms and that have a strong market presence and/or reputational presence among mid and large-sized enterprises.

Included in this Vendor Landscape:

- **Arkoon.**
- **Check Point.**
- **Kaspersky.**
- **Lumension.**
- **McAfee.**
- **Sophos.**
- **Symantec.**
- **Trend Micro.** Strong feature set from a highly viable vendor in the space.

Each vendor offers a different feature set; concentrate on what your organization needs

	Evaluated Features							
	FFE	Encryption	Content Control	Port Control	Patch Mgmt.	App White	URL	Cloud
Arkoon	🟢	🟢	🟡	🟢	🟡	🟢	🟢	🟢
Check Point	🟢	🟢	🔴	🟢	🔴	🟢	🔴	🔴
Kaspersky	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🔴
Lumension	🟡	🟢	🟡	🟢	🟢	🟢	🔴	🔴
McAfee	🔴	🔴	🟡	🔴	🟡	🟢	🟢	🟢
Sophos	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢
Symantec (Endpoint Protection)	🔴	🟢	🟡	🔴	🔴	🟢	🟢	🔴
Symantec (Encryption)	🟢	🟢	🟡	🔴	🔴	🔴	🔴	🔴
Trend Micro	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢

Legend 🟢 **=Feature fully present** 🟡 **=Feature partially present/pending** 🔴 **=Feature absent**

Balance individual strengths to find the best fit for your enterprise

	Product					Vendor				
	Overall	Features	Usability	Afford.	Arch.	Overall	Viability	Strategy	Reach	Channel
Arkoon	◑	●	◑	◑	◔	◑	◕	◑	◑	◑
Check Point*	◔	◔	◑	○	◔	◕	◑	◑	◕	●
Kaspersky	◕	◕	●	◑	●	◕	◕	◕	◑	◕
Lumension	◑	◑	◕	◔	●	◑	◑	◕	◑	◑
McAfee*	◑	◑	◕	○	●	●	●	◕	●	●
Sophos*	●	●	◕	●	●	◕	◕	◕	◕	◕
Symantec (Endpoint Protection)*	◑	◑	●	○	◕	●	●	◕	●	◕
Symantec (Encryption)*	◔	◔	◔	○	◕	●	●	◕	●	◕
Trend Micro	●	●	●	◑	●	◕	●	◕	●	◕

Legend ● **=Exemplary** ◕ **=Good** ◑ **=Adequate** ◔ **=Inadequate** ○ **=Poor**

*The vendor declined to provide pricing and publicly available pricing could not be found.